IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A portable data storage device comprising:

a non-volatile memory to store data[[,]]--;--

an interface section to receive ~~data~~ a command from and transmit the data to a host,

a master control unit to transfer the data ~~to and~~ from the non-volatile memory[[,]]--;-- and

an integrated circuit to generate at least one key,

wherein the portable data storage device is arranged, upon receiving [[a]] the command from the host requesting the data stored in the non-volatile memory, the data stored prior to receiving the command, to generate the at least one key, to encrypt the generated key using a secret key that is permanently stored in the portable storage device, and to transmit the encrypted key and the requested data stored in the non-volatile memory to the host using the interface section, wherein the secret key is permanently stored within the portable storage device prior to the generating at least one key, and

wherein the portable data storage device is further arranged to receive from the host a digital signature based on the generated key and the requested data transmitted to the host from the portable storage device, ~~for use in verifying~~ the portable storage device, based on the digital signature, to verify that the requested data has been correctly received by the host.

2. (Canceled)

3. (Previously Presented) The portable data storage device according to claim 1 wherein the digital signature is produced by hashing the received data to generate a hash result, and encrypting the hash result using the generated key.

4. (Previously Presented) The portable data storage device according to claim 1 wherein the generated key is one key of a public key/private key pair.

5. (Previously Presented) The portable data storage device according to claim 4 wherein the verification of the digital signature is performed in the portable data storage device using the public key.

6. (Canceled)

7. (Currently Amended) The portable data storage device according to claim [[6]] 1 wherein the requested data includes both data present in the non-volatile memory, and also biometric data obtained from a biometric sensor of the portable data storage device.

8. (Previously Presented) The portable data storage device according to claim 1 arranged to transmit the requested data in an encrypted form.

9. (Previously Presented) The portable data storage device according to claim 1, further comprising:

a biometric sensor; and

a verification engine for granting access to data stored in the portable data storage device based on a biometric verification of the user's identity by comparison of biometric data received using the biometric sensor with pre-stored biometric data.

10. (Previously Presented) The portable data storage device according to claim 1 including a compression algorithm for exploiting any redundancy in data received by the portable data storage device to compress it before storing it in the non-volatile memory, and a decompression engine to regenerate the data before it is transmitted from the portable data storage device.

11. (Previously Presented) The portable data storage device according to claim 1 in which the interface section includes a USB connector and a USB interface device.

12. (Previously Presented) The portable data storage device according to claim 11 in which the connector is a USB plug integral with the portable data storage device.

13. (Previously Presented) The portable data storage device according to claim 1 in which the interface section is for wireless communication with the host.

14. (Previously Presented) The portable data storage device according to claim 1 having a housing, the housing including a narrowed end for use as a pointer.

15. (Previously Presented) The portable data storage device according to claim 1, further including a camera for generating image data, and/or a microphone for capturing audio data, the master control unit being arranged to store the image data and/or the audio data in the memory.

16. (Currently Amended) A system comprising:

a portable data storage device including

a non-volatile memory to store data,

an interface section to receive ~~data~~ a command from and transmit the data to a host

a master control unit to transfer the data to and from the non-volatile memory, and

integrated circuit for generating at least one key,

the portable data storage device being arranged, upon receiving [[a]] the command from the host requesting the data stored in the non-volatile memory, the data stored prior to receiving the command, to generate the at least one key, to encrypt the generated key using a secret key that is permanently stored in the portable storage device and to transmit the encrypted key and the requested data stored in the non-volatile memory to the host using the interface section, wherein the secret key is permanently stored within the portable storage device prior to the generating at least one key.

wherein the portable data storage device is further arranged to receive from the host a digital signature based on the generated key and the requested data transmitted to the host from the portable storage device, ~~for use in verifying~~ the portable storage device, based on the digital signature, to verify that the requested data has been correctly received by the host; and

a host computer, the host computer being arranged to transmit [[a]] the command to the portable data storage device using the interface section to request the data.

17. (Previously Presented) The system according to claim 16 wherein the generated key is one key of a public key/private key pair, and the host is arranged to generate a digital signature using the private key and the requested data.

18. (Canceled)

19. (Currently Amended) A method of transferring data from a portable data storage device to a host, the host and the portable data storage device each having a permanently stored secret key, the method comprising the steps of:

the portable data storage device receiving an instruction from the host requesting the data stored in a non-volatile memory of the portable data storage device, wherein the data is stored prior to receiving the instruction;

the portable data storage device generating at least one key;

the portable data storage device encrypting the generated key using the secret key permanently stored in the portable data storage device, wherein the secret key is permanently stored within the portable storage device prior to the generating at least one key;

the portable data storage device obtaining the requested data from the non-volatile memory and the portable data storage device transmitting to the host the requested data and the encrypted key;

the host decrypting the encrypted key using the secret key permanently stored in the host;

the host generating a digital signature based on the decrypted key and the requested data;

the host transmitting the digital signature from the host to the portable data storage device; and

the portable data storage device using the digital signature to verify that the requested data has been correctly received by the host.

20. (Canceled)

21. (Previously Presented) The method according to claim 19 wherein the host generates the digital signature using the private key and the requested data.

22. (Previously Presented) The method according to claim 19 in which the digital signature is produced by hashing the received data to generate a hash result, and encrypting the hash result using the generated key.

23. (Previously Presented) The method according to claim 19 in which the generated key is a private key of a public key/private key pair.

24. (Previously Presented) The method according to claim 23 in which the verification of the digital signature is performed in the portable data storage device using the public key.

25. (Canceled)

26. (Canceled)

27. (Previously Presented) The method according to claim 19 in which the requested data includes both data present in the memory, and also biometric data obtained from a biometric sensor of the portable data storage device.

28. (Previously Presented) The method according to claim 19, in which the requested data is transmitted from the portable data storage device to the host in an encrypted form.

29. (Previously Presented) The method according to claim 19, further comprising verifying a user's identity by comparison of biometric data received using a biometric sensor with pre-stored biometric data, and upon this verification for granting access to the data stored in the portable data storage device.

30. (Previously Presented) The method according to claim 19, including:

the portable data storage device receiving data from the host, the portable data storage device exploiting any redundancy in the data to compress it, and the portable data storage device storing the data in the non-volatile memory; and

upon the data being requested by the host, regenerating the data and transmitting it from the portable data storage device.